Your Feedback Please

We always want you to feel that you made the right decision to use our products. If you have suggestions, comments, compliments or complaints about our products, documentation, or support, please write or call us.

How to Contact Us

ProSoft Technology, Inc.
+1 (661) 716-5100
+1 (661) 716-5101 (Fax)
www.prosoft-technology.com
support@prosoft-technology.com

PLX35-NB2 User Manual
May 8, 2020

ProSoft Technology®, is a registered copyright of ProSoft Technology, Inc. All other brand or product names are or may be trademarks of, and are used to identify products and services of, their respective owners.

In an effort to conserve paper, ProSoft Technology no longer includes printed manuals with our product shipments. User Manuals, Datasheets, Sample Ladder Files, and Configuration Files are provided at our website:
www.prosoft-technology.com

For professional users in the European Union
If you wish to discard electrical and electronic equipment (EEE), please contact your dealer or supplier for further information.

Warning – Cancer and Reproductive Harm – www.P65Warnings.ca.gov

Content Disclaimer

This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither ProSoft Technology nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. Information in this document including illustrations, specifications and dimensions may contain technical inaccuracies or typographical errors. ProSoft Technology makes no warranty or representation as to its accuracy and assumes no liability for and reserves the right to correct such inaccuracies or errors at any time without notice. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without express written permission of ProSoft Technology. All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components. When devices are used for applications with technical safety requirements, the relevant instructions must be followed. Failure to use ProSoft Technology software or approved software with our hardware products may result in injury, harm, or improper operating results. Failure to observe this information can result in injury or equipment damage.

Copyright © 2020 ProSoft Technology, Inc. All Rights Reserved.
Printed documentation is available for purchase. Contact ProSoft Technology for pricing and availability.
**Important Installation Instructions**

Power, Input, and Output (I/O) wiring must be in accordance with Class I, Division 2 wiring methods, Article 501-4 (b) of the National Electrical Code, NFPA 70 for installation in the U.S., or as specified in Section 18-1J2 of the Canadian Electrical Code for installations in Canada, and in accordance with the authority having jurisdiction. The following warnings must be heeded:

**WARNING** - EXPLOSION HAZARD - SUBSTITUTION OF COMPONENTS MAY IMPAIR SUITABILITY FOR CLASS I, DIV. 2;

**WARNING** - EXPLOSION HAZARD - WHEN IN HAZARDOUS LOCATIONS, TURN OFF POWER BEFORE REPLACING OR WIRING MODULES

**WARNING** - EXPLOSION HAZARD - DO NOT DISCONNECT EQUIPMENT UNLESS POWER HAS BEEN SWITCHED OFF OR THE AREA IS KNOWN TO BE NON-HAZARDOUS.

**Class 2 Power**

**Agency Approvals and Certifications**

Please visit our website: [www.prosoft-technology.com](http://www.prosoft-technology.com)
Contents

Your Feedback Please ............................................................................................................. 2
How to Contact Us ............................................................................................................... 2
Content Disclaimer ............................................................................................................. 2
Important Installation Instructions ...................................................................................... 3
Agency Approvals and Certifications .................................................................................. 3

1  Start Here ......................................................................................................................... 6
   1.1 About the PLX35-NB2 Network Bridge .................................................................... 6
       1.1.1 Specifications ................................................................................................. 7
   1.2 PLX35-NB2 Package Contents ............................................................................. 8
   1.3 Jumper Information ............................................................................................... 8
   1.4 Failover and Automatic Backup & Factory Reset ................................................... 9
       1.4.1 Failover .......................................................................................................... 9
       1.4.2 Automatic Backup & Factory Reset ............................................................. 9

2  Quick Start ....................................................................................................................... 10
   2.1 Local Configuration .............................................................................................. 10
   2.2 ProSoft Connect Setup and Configuration .......................................................... 10

3  Installing the PLX35-NB2 ............................................................................................ 11
   3.1 LED Indicators ..................................................................................................... 12

4  Local Configuration using the PLX35-NB2 Configuration Webpage ......................... 14
   4.1 Connecting to the PLX35-NB2 Webpage ............................................................. 14
   4.2 Using the Overview Tab ....................................................................................... 15
   4.3 Setting Gateway Configuration Parameters ...................................................... 16
       4.3.1 Open Source Software and License Information .......................................... 19
   4.4 Configuring Login Credentials .......................................................................... 21
       4.4.1 Initial / Factory Reset Login ........................................................................ 23
   4.5 File Relay ............................................................................................................. 26
       4.5.1 Example #1: Transferring Files across Segmented Networks Using FTP ...... 30
       4.5.2 Example #2: Transferring Files Across Segmented Networks Using SFTP .... 35
   4.6 SD Card ............................................................................................................... 40
   4.7 Viewing Gateway Log file Activity .................................................................... 42
   4.8 Importing a Configuration File .......................................................................... 43
   4.9 Exporting a Configuration File ......................................................................... 44
   4.10 Updating the Firmware ...................................................................................... 45
   4.11 Rebooting the Gateway .................................................................................... 46
   4.12 Factory Reset ..................................................................................................... 47

5  Cloud-based Management Using ProSoft Connect ....................................................... 49
   5.1 Login and Activate ProSoft Connect .................................................................... 49
   5.2 Creating and Connecting a new VPN Client ......................................................... 53
       5.2.1 Verifying the VPN Connection .................................................................... 57
   5.3 Using ProSoft Connect to Configure the PLX35-NB2 ......................................... 59
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4 Adding Team Members</td>
<td>60</td>
</tr>
<tr>
<td>5.4.1 Editing Team Member Access</td>
<td>62</td>
</tr>
<tr>
<td>5.5 Changing Firmware</td>
<td>63</td>
</tr>
<tr>
<td><strong>6 Ethernet Cable Specifications</strong></td>
<td><strong>67</strong></td>
</tr>
<tr>
<td>6.1 Ethernet Cable Configuration</td>
<td>67</td>
</tr>
<tr>
<td><strong>7 Support, Service &amp; Warranty</strong></td>
<td><strong>68</strong></td>
</tr>
<tr>
<td>7.1 Contacting Technical Support</td>
<td>68</td>
</tr>
<tr>
<td>7.2 Warranty Information</td>
<td>69</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td><strong>70</strong></td>
</tr>
</tbody>
</table>
1 Start Here

1.1 About the PLX35-NB2 Network Bridge

The PLX35-NB2 Network Bridge is the ideal solution for system integrators, machine builders, and OEMs requiring remote system access for commissioning, troubleshooting, or network maintenance.

During the commissioning phase, a network bridge is deployed on site with automation equipment. Once the equipment is installed and ready for configuration and programming, the bridge allows the user to remotely access the network to commission, maintain, and troubleshoot the system, thereby reducing travel time costs.

By deploying a network bridge to an existing network, the network bridge allows access from anywhere by authorized personnel. In the event of unscheduled downtime, an authorized user can connect to the network to minimize downtime and loss of profit.

Module configuration and remote connections are accomplished through ProSoft Connect, ProSoft Technology’s secure, cloud-native platform for the Industrial Internet of Things (IoT).

The PLX35-NB2 allows users to:
- Securely connect to remote devices from any PC without having to use a 3rd-party software application
- Locally control the VPN connection through an EtherNet/IP® message.

The PLX35-NB2 provides 2 Ethernet ports. One port is used for the local network requiring remote access. The second port is used to connect to the internet.
# 1.1.1 Specifications

## Power

<table>
<thead>
<tr>
<th>Power</th>
<th>24 VDC nominal, 10 to 36 VDC allowed, Positive, Negative, and GND terminals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Connector</td>
<td>Three pin, screw terminal, screw retention, black</td>
</tr>
<tr>
<td>Current Load</td>
<td>24 VDC nominal @300 mA</td>
</tr>
</tbody>
</table>

## Internal Specs

<table>
<thead>
<tr>
<th>EtherNet/IP</th>
<th>Supports local control of VPN access through MSG instruction.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Ports</td>
<td>HTTP or HTTPS ports 8080</td>
</tr>
</tbody>
</table>

## Physical

<table>
<thead>
<tr>
<th>Enclosure</th>
<th>Extruded aluminum with DIN clip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimensions (H x W x D)</td>
<td>5.52 x 2.06 x 4.37 in</td>
</tr>
<tr>
<td></td>
<td>14.01 x 5.24 x 11.09 cm</td>
</tr>
<tr>
<td>Shock</td>
<td>IEC 60068-2-27; 20G @ 11ms (Operational)</td>
</tr>
<tr>
<td></td>
<td>IEC 60068-2-27; 30G @ 11ms (Non-Operational)</td>
</tr>
<tr>
<td>Vibration</td>
<td>IEC 60068-2-6; 10G, 10 to 150 Hz</td>
</tr>
<tr>
<td>Ethernet Port</td>
<td>(2) 10/100 Base-T, RJ45 connector</td>
</tr>
</tbody>
</table>

## Environmental

<table>
<thead>
<tr>
<th>Operating Temperature</th>
<th>IEC 60068: -22°F to +158°F (-30°C to +70°C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Humidity</td>
<td>IEC 60068-30; 5% to 95%, with no condensation</td>
</tr>
<tr>
<td>External Power</td>
<td>10 to 30 VDC</td>
</tr>
<tr>
<td>Peak Power Consumption</td>
<td>&lt; 6W</td>
</tr>
</tbody>
</table>
1.2 PLX35-NB2 Package Contents

The following components are included with the PLX35-NB2 and are required for installation and configuration.

Important: Before beginning the installation, please verify all of the following items are present.

<table>
<thead>
<tr>
<th>Qty.</th>
<th>Part Name</th>
<th>Part Number</th>
<th>Part Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PLX35-NB2 Network Bridge</td>
<td>PLX35-NB2</td>
<td>2-port Network Bridge</td>
</tr>
<tr>
<td>1</td>
<td>2-pin Power Connector</td>
<td>002-0116</td>
<td>Power Connector</td>
</tr>
</tbody>
</table>

If any of these components are missing, please contact ProSoft Technology Technical Support for replacement parts. See Contacting Technical Support (page 68).

1.3 Jumper Information

The module has one visible set of jumper pins on the back of the gateway. These pins should only be jumped/shunted when resetting the gateway back to factory defaults.

To perform a factory reset:

1. Set the jumper on both pins and power-cycle the module.
2. Wait until the FLT, CFG and ERR LED’s flash in a reverse-clockwise direction (the gateway should boot twice by then).
3. You will notice all the LED’s flashing twice (except interface LED’s).
4. Remove the jumper and wait for the gateway to finish the power-cycle.
5. When the factory reset has finished, the CFG LED flashes.
1.4 Failover and Automatic Backup & Factory Reset

1.4.1 Failover

The Failover process provides a recovery mechanism whenever a serious malfunction renders the main filesystem inoperable.

If the system fails to boot up (all LEDs are solid on) 4 times in a row, on the 5th boot up the gateway will enter a failover state (the FLT LED is solid red and the CFG LED blinks amber). While in this state, the PLX35-NB2 can be accessible using its default configuration. A new upgrade can be performed on the gateway which should fix the serious malfunction that led to the failover state.

1.4.2 Automatic Backup & Factory Reset

If the system fails to boot up (all LEDs are solid on) 10 times in a row, on the 11th boot up the gateway tries to restore the backup firmware and configuration. The backup firmware and configuration are in place before the last upgrade was performed.

If the backup restore procedure has performed correctly, only the PWR LED will be lit upon boot up.

The automatic factory reset process takes place when the PLX35-NB2 needs to return to the default configuration. This is because the backup restore process has not succeeded. After this process is completed, it will run the factory default image with the default configuration, in an out-of-the-box condition. In this case, there is no need to use a jumper to perform a factory reset.

If the factory reset has performed correctly, the CFG LED will blink amber.
2 Quick Start

2.1 Local Configuration

<table>
<thead>
<tr>
<th>Task</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the module</td>
<td>11</td>
</tr>
<tr>
<td>Connect to the PLX35-NB2 webpage</td>
<td>14</td>
</tr>
<tr>
<td>Set gateway configuration parameters</td>
<td>16</td>
</tr>
<tr>
<td>Configure login credentials</td>
<td>21</td>
</tr>
<tr>
<td>Update firmware</td>
<td>45</td>
</tr>
</tbody>
</table>

2.2 ProSoft Connect Setup and Configuration

ProSoft Connect allows you to remotely configure, maintain, and troubleshoot the gateway.

<table>
<thead>
<tr>
<th>Task</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain an activation key and login to ProSoft Connect</td>
<td>49</td>
</tr>
<tr>
<td>Create a VPN client</td>
<td>53</td>
</tr>
<tr>
<td>Establish a VPN Connection</td>
<td>53</td>
</tr>
<tr>
<td>Perform configuration functions in ProSoft Connect</td>
<td>59</td>
</tr>
<tr>
<td>Add Team Members</td>
<td>60</td>
</tr>
<tr>
<td>Change Firmware if required</td>
<td>63</td>
</tr>
</tbody>
</table>
3 Installing the PLX35-NB2

Mount the PLX35-NB2 such that:

- There is easy access for the cables to ensure that they are not bent, constricted, in close proximity to high amperage, or exposed to extreme temperatures.
- The LEDs on the front panel are visible for troubleshooting and verifying the gateway status.
- There is adequate airflow around the gateway, but also protected from direct exposure to the elements, such as sun, rain, and dust.

Caution: The PLX35-NB2 is in a hardened case, and is designed for use in industrial and extreme environments; however, unless you are using cables expressly designed for such environments, the cables can fail if exposed to the same conditions the PLX35-NB2 can withstand.
### 3.1 LED Indicators

The following tables describe the diagnostic LEDs on the PLX35-NB2.

<table>
<thead>
<tr>
<th>LED</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGMT</td>
<td>Off</td>
<td>The module cannot reach the internet and is not managed by ProSoft Connect (default).</td>
</tr>
<tr>
<td></td>
<td>Flashing Green</td>
<td>The module can reach the internet.</td>
</tr>
<tr>
<td></td>
<td>Solid Green</td>
<td>The module is managed by a ProSoft Connect account.</td>
</tr>
<tr>
<td></td>
<td>Solid Red</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Flashing Red</td>
<td>The module is configured to be managed by ProSoft Connect but cannot reach ProSoft Connect.</td>
</tr>
<tr>
<td></td>
<td>Alternating Red/Green</td>
<td>N/A</td>
</tr>
<tr>
<td>VPN</td>
<td>Off</td>
<td>ProSoft Connect is not enabled (default).</td>
</tr>
<tr>
<td></td>
<td>Flashing Green</td>
<td>VPN is possible (normal).</td>
</tr>
<tr>
<td></td>
<td>Solid Green</td>
<td>A VPN tunnel is established.</td>
</tr>
<tr>
<td></td>
<td>Solid Red</td>
<td>The module is managed by ProSoft Connect and EIP has disabled VPN tunneling.</td>
</tr>
<tr>
<td></td>
<td>Flashing Red</td>
<td>VPN connection failed.</td>
</tr>
<tr>
<td></td>
<td>Alternating Red/Green</td>
<td>N/A</td>
</tr>
<tr>
<td>PWR (Power)</td>
<td>Off</td>
<td>Power is not connected to the power terminals or source is insufficient to properly power the module.</td>
</tr>
<tr>
<td></td>
<td>Solid Green</td>
<td>Sufficient power is connected to the power terminals.</td>
</tr>
<tr>
<td>FLT (Fault)</td>
<td>Off</td>
<td>Normal operation</td>
</tr>
<tr>
<td></td>
<td>Solid Red</td>
<td>A critical error has occurred. Program executable has failed or has been user-terminated and is no longer running. Press the Reset button or cycle power to clear the error.</td>
</tr>
<tr>
<td>CFG</td>
<td>Off</td>
<td>Normal operation</td>
</tr>
<tr>
<td></td>
<td>Flashing Amber</td>
<td>The module has no configuration.</td>
</tr>
<tr>
<td></td>
<td>Solid Amber</td>
<td>The module is in configuration mode. Either a configuration error exists, or the configuration file is currently being downloaded or read. After power-up or after the Reset button is pressed, the configuration is read and the module implements the configuration values and initializes the hardware.</td>
</tr>
<tr>
<td>ERR</td>
<td>Off</td>
<td>Normal operation</td>
</tr>
<tr>
<td></td>
<td>Flashing Amber</td>
<td>An error condition has been detected and is occurring on one of the application ports. Check configuration and troubleshoot for communication errors.</td>
</tr>
<tr>
<td></td>
<td>Solid Amber</td>
<td>The ERR LED is cleared on receipt of a well-formed allowed packet. On receipt of data packet containing an unsupported protocol, the LED is lit. If the LED is solid, a large number of errors are occurring on one or more ports (network communication errors).</td>
</tr>
</tbody>
</table>
## Ethernet Port LEDs

<table>
<thead>
<tr>
<th>LED</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 Mbit</td>
<td>Off</td>
<td>No activity on the port</td>
</tr>
<tr>
<td></td>
<td>Flashing Amber</td>
<td>The Ethernet port is actively transmitting or receiving data.</td>
</tr>
<tr>
<td>LNK/ACT</td>
<td>Off</td>
<td>No physical connection is detected. No Ethernet communication is possible. Check wiring and cables.</td>
</tr>
<tr>
<td></td>
<td>Solid Green</td>
<td>Physical network connection detected. This LED must be ON (solid) for Ethernet communication to be possible.</td>
</tr>
</tbody>
</table>
4 Local Configuration using the PLX35-NB2 Configuration Webpage

The PLX35-NB2 contains a browser-based configuration webpage used for configuration. The following sections describe the configuration process.

4.1 Connecting to the PLX35-NB2 Webpage

1. Ensure that the module is connected to the network through the LAN port.
2. Apply power to the module.
3. To log into the PLX35-NB2 configuration webpage through the network, your PC must be able to connect to the PLX35-NB2. The default IP address of the PLX35-NB2 is 192.168.0.250. If your PC is on a different subnet, temporarily set the IP address of your PC to 192.168.0.xxx with a subnet of 255.255.255.0 (where xxx is an available address on the network).

<table>
<thead>
<tr>
<th>IP address:</th>
<th>192.168.0.250</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet mask:</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

**Note:** You can also use ProSoft Discovery Service to discover the IP address. You can download and install ProSoft Discovery Services from the ProSoft website at [www.prosoft-technology.com](http://www.prosoft-technology.com).

4. Open a web browser on your PC and enter the PLX35-NB2 default address of: **192.168.0.250:8080**. Minimum browser requirements include Chrome 58, Firefox 54, and Internet Explorer 10.
5. Once the PLX35-NB2 configuration webpage opens, enter the **USERNAME** and **PASSWORD** to log in. The default **USERNAME** is admin and the default **PASSWORD** is password.

**Important:** For security purposes, you must change the default user name and password after initial login or factory reset. See Initial / Factory Reset Login on page 23.
6 After you successfully log in, the configuration webpage displays the **Overview** tab.

This page allows you to:
- View Performance Information
- View Device Details
- Update Firmware
- Manually enter a custom date and time

4.2 Using the Overview Tab

The **Overview** tab contains performance information as well as device details, access information, and module location information.

In addition, this page allows you to make firmware updates to the gateway. You can view this tab at any time by simply clicking on the **Overview** tab.

**Tip:** This tab provides an *Activation Code* that allows you to take advantage of configuring and maintaining your gateway using ProSoft Connect. See *Cloud-based Maintenance using ProSoft Connect* on page 49 for details on using this code.
4.3 Setting Gateway Configuration Parameters

1. Click on the **Gateway** tab.

2. Use the following tables to enter the appropriate parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway Name</td>
<td>Enter a name for this gateway.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description to describe the gateway. For example, <em>Network Bridge - Bakersfield</em>.</td>
</tr>
<tr>
<td>Address</td>
<td>Enter the street address of the gateway (i.e., where the gateway resides)</td>
</tr>
<tr>
<td>Advanced configuration (link)</td>
<td>This link allows you to provide GPS coordinates of the gateway’s location.</td>
</tr>
</tbody>
</table>
### Local Area Network

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>Enter the IP address of the gateway. This is a static IP address. The default IP address is 192.168.0.250. (The netmask is always 255.255.255.0).</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>Use this parameter to enable or disable DHCP. The default is <strong>Disabled</strong>. If you want to use a DHCP server to select an IP, select <strong>Enabled</strong>. Selecting <strong>Enabled</strong> displays a number of additional DHCP-related parameters.</td>
</tr>
<tr>
<td>DHCP Lease Time</td>
<td>Allows you to select lease times in hour, minutes, or seconds. This is the amount of time an IP address remains available on a particular device before releasing the IP address for use by another device.</td>
</tr>
<tr>
<td>DHCP Lease Units</td>
<td>Allows you to specify Hours and Minutes and works in conjunction with <strong>DHCP Lease Time</strong>.</td>
</tr>
<tr>
<td>DHCP Pool Low</td>
<td>DHCP uses a pool of assigned addresses that are available to requests. <strong>DHCP Pool Low</strong> allows you to set the last octet to the low end number of the pool. (See example below)</td>
</tr>
<tr>
<td>DHCP Pool High</td>
<td>DHCP uses a pool of assigned addresses that are available for use. <strong>DHCP Pool High</strong> allows you to specify the high-end last octet of the pool.</td>
</tr>
</tbody>
</table>

- **DHCP Lease Time** - Allows you to select lease times in hour, minutes, or seconds. This is the amount of time an IP address remains available on a particular device before releasing the IP address for use by another device.
- **DHCP Lease Units** - Allows you to specify Hours and Minutes and works in conjunction with **DHCP Lease Time**.
- **DHCP Pool Low** - DHCP uses a pool of assigned addresses that are available to requests. **DHCP Pool Low** allows you to set the last octet to the low end number of the pool. (See example below)
- **DHCP Pool High** - DHCP uses a pool of assigned addresses that are available for use. **DHCP Pool High** allows you to specify the high-end last octet of the pool.

For example:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Pool Low</td>
<td>192.168.72.100</td>
</tr>
<tr>
<td>DHCP Pool High</td>
<td>192.168.72.249</td>
</tr>
</tbody>
</table>

This example specifies that the range of addresses that may be used is between 192.168.72.100 through 192.168.72.249.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP</td>
<td>This parameter specifies whether or not the Network Time Protocol (NTP) is enabled or disabled. The default is <strong>Enabled</strong>. If <strong>Disabled</strong>, the following two parameters are not present.</td>
</tr>
<tr>
<td>NTP Server 1</td>
<td>Default set to: <strong>0.us.pool.ntp.org</strong>. If you wish to use a different NTP server, enter it here.</td>
</tr>
<tr>
<td>NTP Server 2</td>
<td>Default set to: <strong>1.us.pool.ntp.org</strong>. If you wish to use a different NTP server, enter it here.</td>
</tr>
<tr>
<td>NTP Server 3</td>
<td>Default set to: <strong>2.us.pool.ntp.org</strong>. If you wish to use a different NTP server, enter it here.</td>
</tr>
<tr>
<td>NTP Mode</td>
<td>Default is <strong>Client</strong>. You can change this to Client/Server mode.</td>
</tr>
</tbody>
</table>
### Wide Area Network (WAN)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Client</td>
<td>This is set to <strong>Enabled</strong> by default. If your administrator wants to assign a static IP, this should be set to <strong>Disabled</strong>. If <strong>Disabled</strong>, you must supply the following information: <strong>IP</strong> - The IP address assigned to the WAN port. <strong>Subnet</strong> - Enter the subnet address. <strong>Gateway</strong> - Enter the gateway address for this subnet. <strong>DNS 1</strong> - Enter the Domain Name Server IP provided to your system. <strong>DNS 2</strong> - Enter the backup Domain Name Server IP provided to your system.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>If the gateway is part of a VLAN, enter the VLAN ID.</td>
</tr>
</tbody>
</table>

3. Click the **APPLY CHANGES** button when complete.
4.3.1 Open Source Software and License Information

To view a list of the software and licenses contained in the PLX35-NB2, click on the LICENSES link at the bottom of the Gateway tab.

A list of the Open Source software and its license terms are displayed:
License Details:

Each entry can be expanded:
4.4 Configuring Login Credentials

The gateway is shipped with the following login defaults:

User: admin
Password: password

The Access tab allows you to change the defaults.

1 Click on the Access tab to view the Access page.

This page allows you to set up the users that can manage and configure this gateway. The Advanced Configuration link allows you to restrict access based on user.

2 Enter a user name.
3 Enter a password.
4 Confirm the password by retyping it.
Advanced Configuration

1. Click on the *Advanced Configuration* link.

2. Select the *Web Protocol*. Select **HTTP** or **HTTPS**.
3. Choose the port depending on what protocol is selected.
4. Click **APPLY CHANGES** when complete.
4.4.1 Initial / Factory Reset Login

This procedure is used for brand new units, or resetting the PLX35-NB2 to the default configuration. The default credentials are as follows:

**User:** admin  
**Password:** password

**Note:** Beginning with PLX35-NB2 firmware v1.5, this process requires you to change the default password on initial/reset login.

1. Connect to the PLX35-NB2 webpage using the default credentials.

![Login Screen](image)

2. After logging in, the Access tab will be displayed to change the password.

**Note:** The other tabs are not available until the password change is complete. This step cannot be skipped.
3. Select a password that is compatible with the following rules:
   - Between 8 and 40 characters
   - At least one upper case letter
   - At least one lowercase letter
   - Contains at least one digit (0 through 9)
   - Contains at least one special character (!@#$%^&*()_+=~)

4. Re-enter the new password in the Confirm Password field.

5. After confirming the new password in the Confirm Password field, click the Apply changes button in the top right corner of the page.

6. After the changes are applied, you will be logged out and redirected to the login page.
After logging in using the username and the new password, future password changes can be done from the Access tab as in the Configuring Login Credentials section on page 21.
4.5 File Relay

The LAN and WAN ports on the PLX35-NB2 are physically isolated. The File Relay functionality enables simple and secure transfer of files across segmented networks.

For example, if the customer would like to back up all of their OT equipment configuration files on the server without wanting to create a link between the IT and OT network, the PLX35-NB2 can be used to segment between the two networks.

The File Relay tab allows you to use the SD card port on the device as a temporary storage medium for large files that can be automatically transferred to a remote location.

Files can be copied to the PLX35-NB2 SD card from a FTP/SFTP Client. The files can then transferred to a remote FTP/SFTP Server, or via ProSoft Connect.

*Note that the option to transfer the files to ProSoft Connect is currently not operational. It will be functional on the next ProSoft Connect Release.
1 In the *Incoming* section of the *File Relay* tab, select the **FTP** or **SFTP** Protocol to enable FTP or SFTP Incoming file transfer.

2 Use the following tables to enter the appropriate parameters:

### Incoming

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Protocol** | FTP (File Transfer Protocol)  
SFTP (Secure File Transfer Protocol) |
| **User** | The user name is for uploading files through FTP to the module's SD card. The default value is `f-relay`. |
| **Password** | Password for FTP access. The password must have at least 8 characters, contain at least one uppercase letter, one lowercase letter, and one special character. |

### Outgoing

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Protocol** | Protocol of the server used as final destination for the File Relay.  
- Supported protocols for upload are FTP/SFTP/ProSoft Connect  
**Note:** ProSoft Connect not available at this time. |
| **URL** | URL of the server used as final destination for the File Relay.  
- Supported protocols for upload are FTP/SFTP/ProSoft Connect  
- For FTP the format is specified in the field: `ftp://user@host:port/path/`  
- For SFTP the format is: `sftp://user@host:port/path/` |
| **Password** | Password used to upload to the remote server. You can view the configured value by pressing the "eye" button.  
- Password is used only for FTP  
- This field is greyed out for SFTP  
- This field is removed for ProSoft Connect |
<table>
<thead>
<tr>
<th>Host Key</th>
<th>Public Key that authenticates SFTP Server and proves its identity to PLX35-NB2 client. This should be copied from SFTP Server and pasted here.</th>
</tr>
</thead>
</table>
|          | **Used only for SFTP**  
|          | **This field is greyed out for FTP**  
|          | **This field is removed for ProSoft Connect**  
|          | **Keys supported: RSA 2048, RSA 3072, RSA 4096, Ed25519 255, ECDSA nistp256, ECDSA nistp384, ECDSA nistp521**  
|          | **Keys unsupported: DSA 1024, ECDSA secp256k1**  
|          | **ssh-rsa**  
|          | AAAAB3NzaC1yc2EAAAADAQABAADBggC4oa5f2L6+X/1Jz5+YfY3hpmA==  
|          | **ecdsa-sha2-nistp384**  
|          | AAAAB3NzaC1yc2EAAAADAQABAAABAQCSi6Q3mghw0d3o0wudz1Pz+8GQ==  
|          | **Standard SSH2 format is NOT supported:**  
|          | ---- BEGIN SSH2 PUBLIC KEY ----  
|          | AAAAB3NzaC1yc2EAAAADAQABAADQaEElwQxIwK CBC3c6eRsKUnOazfUWHLtCTZB49sx  
|          | ---- END SSH2 PUBLIC KEY ----  

**OpenSSH format:**

```
AAAAB3NzaC1yc2EAAAADAQABAAABGggC4oa5f2L6+X/1Jz5+YfY3hpmA==
AAAAB3NzaC1yc2EAAAADAQABAADBggC4oa5f2L6+X/1Jz5+YfY3hpmA==
```

**Standard SSH2 format:**

```
-----BEGIN SSH2 PUBLIC KEY-----
AAAAB3NzaC1yc2EAAAADAQABAADBggC4oa5f2L6+X/1Jz5+YfY3hpmA==
 AAAAB3NzaC1yc2EAAAADAQABAADBggC4oa5f2L6+X/1Jz5+YfY3hpmA==
-----END SSH2 PUBLIC KEY-----
```
**Note:** Host Key will be removed from the outgoing server configuration upon downgrade from PLX35-NB2 1.5 release to any older firmware.

### SSH-Key

SSH-Key is the public key that authenticates the SFTP Server user for file transfer. Once generated, it should be copied to the SFTP Server as a .pub file and associated with the designated user. The SSH-Key pair generation takes place the first time it is requested. Subsequent requests return the same public key.

SSH keys will be removed upon gateway factory reset.
- Used only for SFTP
- This field is greyed out for FTP
- This field is removed for ProSoft Connect

**Daily Upload Time**

The upload time, shown in the Local UI is UTC – similar with the time on the Overview page. Default time value is 03:00.

3 Click **APPLY CHANGES** when complete.
4.5.1 Example #1: Transferring Files across Segmented Networks Using FTP

This example shows an incoming FTP to an outgoing FTP.

- On the LAN port, the PLX35-NB2 acts as a FTP Server for the incoming files to a WinSCP Client. The files will be temporarily stored in the PLX35-NB2 SD card.
- On the WAN port, the PLX35-NB2 acts as a FTP Client to a Filezilla Server. The files are pushed from the PLX35-NB2 to the Filezilla FTP Server.

Filezilla Server
(Resides on a PC)
User: admin
Password: Prosoft12341

WinSCP Client
(Resides on a PC)
User: f-relay
Password: Prosoft12341
1. From the WinSCP Client, open a FTP session to PLX35-NB2 and transfer a few files to the upload folder on the PLX35-NB2 SD card:

2. Click Ok.
3. Log into the FTP Filezilla Server.

**User:** admin
**Password:** Prosoft1234!
**Folder:** C:\FTP_Root)
4 Start the server:

FileZilla Server (127.0.0.1)

FileZilla Server 0.9.60 beta
Copyright 2001-2016 by Tim Kosse tim.kosse@filezilla-project.org
https://filezilla-project.org/
Connecting to server localhost:14147...
Connected, waiting for authentication
Logged on
Warning: FTP over TLS is not enabled, users cannot securely log in.
Retrieving account settings, please wait...
Done retrieving account settings
Retrieving account settings, please wait...
Done retrieving account settings
Retrieving account settings, please wait...
Done retrieving account settings
Creating listen socket on port 21...
Server online
5 At the configured *Daily Upload Time*, set (hh:mm, default is 03:00). The files from the PLX35-NB2 SD card upload folder will be time-stamped (yyyy-mm-dd) and transferred to the FTP Filezilla Server on folder C:\FTP_Root.
4.5.2 Example #2: Transferring Files Across Segmented Networks Using SFTP

This example shows an incoming SFTP to Outgoing SFTP.

- On the LAN port, the PLX35-NB2 acts as a SFTP Server for the incoming files from the WinSCP Client. The files will be temporarily stored on the SD card.
- On the WAN port, the PLX35-NB2 acts as a SFTP Client to a Bitvise Server. The files are pushed from the PLX35-NB2 to the Bitvise SFTP Server.

**Bitvise Server**
(Resides on a PC)

**PLX35-NB2**

**WinSCP Client**
(Resides on a PC)

User: admin
Host Key: Copied from Managed host keys Bitvise to PLX35-NB2
Public Key: Copied from PLX35-NB2
SSH-Key box to Bitvise

User: f-relay
Password: Prosoft1234!
1. From the WinSCP Client, open a SFTP session to PLX35-NB2 and transfer few files to **upload** folder on PLX35-NB2 SD card:
2. On the Bitvise server, managing public keys:
   - Generate a key on Bitvise Manage host keys, export it as OpenSSH format, then copy the key to Host Key box into the PLX35-NB2
   - Generate SSH Key on PLX35-NB2, copy into a .pub file and add it on admin account on Bitvise server
After the Bitvise server is started, set the *Daily Upload Time* (hh:mm, default is 03:00). The files from the PLX35-NB2 SD card **upload** folder will be time-stamped (yyyy-mm-dd) and transferred to PC 2 FTP Bitvise Server on folder C:\SFTP_Root.
4.6 SD Card

The SD Card tab allows you to Eject, Mount, Format, and diagnose the PLX35-NB2 SD Card. You can also optimize the SD Card in this tab.

You can only access the SD Card from a FTP/SFTP Client.

1. Use the following tables to enter the appropriate parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eject</td>
<td>Recommended to be done before manually removing SD Card.</td>
</tr>
<tr>
<td>Mount</td>
<td>This allows the SD card to be visible to the PLX35-NB2. When the SD Card is not 'mounted', it will not be visible to the PLX35-NB2.</td>
</tr>
<tr>
<td>File System Check</td>
<td>Checks the SD Card for errors. This should be used in case the SD Card cannot be mounted. The page will be refreshed after the File System Check process is finished, then the user can manually mount the SD Card using Mount button.</td>
</tr>
<tr>
<td>Format</td>
<td>Removes the data from the SD Card and creates a new file system (FAT32 type).</td>
</tr>
</tbody>
</table>

Note: These options may be greyed out according to the SD card status.

- If the SD Card is not present, the SD Card options are greyed out.
- If the SD Card is not mounted, the EJECT and FORMAT buttons are greyed out.
- If the SD Card is mounted, the MOUNT button is greyed out.
Space Management

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reclaim Space</td>
<td>Automatically cleans up the SD Card. Default value is <strong>Disabled</strong>.</td>
</tr>
<tr>
<td>High Water Mark (%)</td>
<td>The system will start deleting files from the SD Card when this threshold is reached.</td>
</tr>
<tr>
<td>Low Water Mark (%)</td>
<td>The system will delete files from the SD Card until this threshold is reached.</td>
</tr>
</tbody>
</table>

2. Click **APPLY CHANGES** when complete.

**Note:** The High and Low Water Mark values should be based on the size of the SD Card and the sizes of the uploaded files. Setting inappropriate values might cause the deletion of files before the upload is performed.
4.7 Viewing Gateway Log file Activity

1. Click on the **Activity** tab.

Options on this page include search, search filter options, and a Download log file option.

2. Click on the **Download Log File** button to download a .txt file to the download folder of your PC or laptop.

**Note:** Some options that appear in the configuration UI may not be available during management or configuration options within ProSoft Connect.
4.8 Importing a Configuration File

1. Select **IMPORT CONFIGURATION** from the setup icon located in the upper-right corner of any configuration page.

2. Locate and select a configuration file to import and then click the **Import** button.
4.9 Exporting a Configuration File

1. Select **Export Configuration** from the setup icon located in the upper-right corner of any configuration page.

2. The gateway downloads a **tar.gz** file to your PC or laptop. Do not modify this file.
4.10 Updating the Firmware

**Note:** Downgrading to old firmware versions:

- If running firmware version is 1.2.13 or newer, performing a downgrade to versions 1.1.57 or 1.0.24 is not supported.

- If running firmware version is 1.2.31 or newer, performing a downgrade to versions 1.2.13, 1.1.57 or 1.0.24 is not supported.

**Note:** ProSoft Connect can also schedule updates to the latest firmware for multiple PLX35-NB2 gateways.

1. Click the **Setup** icon in the top-right corner of the page and then click **Change Firmware**.

   ![Change firmware dialog](image1)

   This opens the *Change firmware* dialog.

2. Click the **Choose File** button and locate the firmware file.
3. Select the file and click **Open**.
4. Click the **Change** button to load the new firmware.
5. After the firmware update is complete, refresh PLX35-NB2 webpage.
4.11 Rebooting the Gateway

1. Click the **Setup** icon in the upper-right corner of the page and then click **Reboot Gateway**.

   ![Reboot Gateway Dialog](image)

   This opens the *Reboot gateway* dialog.

2. Click the **Reboot** button when ready.
4.12 Factory Reset

The *Factory Reset* option will reset the PLX35-NB2 to its default configuration. All custom configuration changes will be lost after this procedure.

1. Press the cogwheel symbol in the top right corner of the page.

2. In the drop down, select the **Factory reset** option.

3. Click the **FACTORY RESET** button in the pop-up message that appears on the screen.

A pop-up message will indicate the factory reset procedure has begun.
4 After a few minutes, the PLX35-NB2 will be available via its local UI, using the default IP address (192.168.0.250) and the default port (8080).

![Login interface with default credentials]

5 After the factory reset is complete, the first login will be done using the default credentials (admin/password). It will then require you to change the password as shown in the Initial / Factory Reset Login section on page 23.
5 Cloud-based Management Using ProSoft Connect

ProSoft Connect allows you to manage multiple gateways on the network through a secure VLAN tunnel via a webpage. You can perform multiple tasks, including activating, setting up VPN clients, perform configuration and maintenance, and invite team members.

5.1 Login and Activate ProSoft Connect

Obtaining the Activation Key

ProSoft Connect requires that you activate the PLX35-NB2 the first time you use it. You must obtain an activation key from the gateway.

1 Connect your gateway WAN port to a network that can reach the internet. The MGMT LED will flash GREEN if the PLX35-NB2 can reach the internet and is not yet activated.

2 Log in to the module from the LAN port as described in the section entitled “Connecting to the PLX35-NB2 Webpage” (page 14). This takes you to the Overview tab.

3 Under Device Details, click the Activate link to the right of the ProSoft Connect label.

Note: If the gateway is already connected to a ProSoft Connect account, the link reads “Deactivate”.

4 The gateway securely retrieves an alphanumeric activation key from ProSoft Connect that is only valid for three (3) hours. Record this activation key.

Note: The module must be connected to the internet through the WAN port in order for the module to retrieve an activation key.

5 Open a new tab in your web browser, enter www.prosoft.io in the address bar, and then press ENTER.
6 In the ProSoft Connect Login screen, enter your ProSoft Connect login email and password and click LOGIN, or click SIGN UP to create a new account. Login credentials are not interchangeable between ProSoft Connect and the local interface.

7 After you are logged in, you can take a tour of the features of ProSoft Connect by clicking TAKE THE TOUR. Or you can skip the tour to configure the gateway.
8 When ready, activate the PLX35-NB2 within the tour, or you can click on the **ADD GATEWAY** button from the *Gateways* tab.

ProSoft Connect prompts you for the activation key that you recorded earlier. Click **ACTIVATE**.
10 Upon successful activation, the PLX35-NB2 appears on the *Gateways* page.
5.2 Creating and Connecting a new VPN Client

ProSoft Connect uses your native Windows VPN client for secure remote access. The first time you intend to establish a VPN connection, you must set up the client and then connect to it. Initial VPN client configuration is only done once and is described in the following steps. If you already have a ProSoft Connect VPN Client established in your Network Connections folder, you do not need to perform these steps.

Once your PLX35-NB2 is activated, the gateway is displayed on the Gateways page.
1 In the Gateways tab, click on the CONNECT button of the gateway profile.

2 Assign the PC's IP address and subnet mask.
3 The system generates a unique secure one-time use username.

The system generates a unique secure one-time use username.

4 Click the COPY TO CLIPBOARD button to save this username.

5 Click "SHOW ME HOW TO SETUP MY VPN CLIENT." This opens the Set Up VPN Client in ProSoft Connect dialog.
6 Click on the **INITIAL CONFIGURATION (ONE-TIME SETUP)** option. Follow the tutorial to complete the setup. The tutorial also shows you how to connect to the VPN tunnel.

![Initial configuration 1/11](image)

After tunneling to the gateway by pressing Connect, you will see a window showing you the generated username for tunnel access. Copy the username to be used later in setup.

![Username generated](image)

The tunnel has been initiated. We are waiting for you to connect to your PC...
5.2.1 Verifying the VPN Connection

The module on the Gateways page of ProSoft Connect provides a VPN indicator as shown:

You can view the connection status by hovering over the VPN icon or by hovering over the status at the top of the page. See the next section for more details.

This indicator is grayed out if there is no connection established. However, you can hover over this indicator to obtain more information about the connection.

The example above shows that both the gateway and the user are connected to the VPN server.
If only one part of the tunnel connection is established, the indication may appear as shown below:

![VPN Connection Example](image.png)

This example shows a connection between the gateway and the VPN server. However, it shows the user as "Disconnected". In this case, ProSoft Connect may be waiting for the user to provide a user name in order to connect to the VPN.
5.3 Using ProSoft Connect to Configure the PLX35-NB2

All configuration tasks may be performed using ProSoft Connect. You do not need to use the module's internal web server to configure the module or edit existing configurations.

To access configuration parameters, click on the module name.

This opens the gateway's configuration pages.

In addition to the normal features of ProSoft Connect, these configuration pages are exclusive to the PLX35-NB2. The configuration tabs are the same as those described under "Local Configuration using the Gateway's Configuration Webpage" on page 14.
5.4 Adding Team Members

Within ProSoft Connect, you can invite team members to your account. This allows others to securely access the remote site and perform maintenance and configuration functions on the gateway once invites are accepted.

1. Click on the Team icon.

2. Click on the Invite Team Members button located in the upper-right hand corner of the page.
3 The *Invite New Team Member* dialog opens.

![Invite New Team Member dialog](image)

4 Enter the information and the project role of the person you want to invite.

**Note:** An email address can only be associated with one ProSoft Connect account at a time.

5 Modify the *Message* dialog to send a unique message to the invitees.

6 When you are done, click the **SEND INVITATION** button. You should receive an “invitation sent successfully” message if the email address was valid. You can edit a member’s access rights once the invite is sent.
5.4.1 Editing Team Member Access

As an administrator, you can control the type of access rights assigned to your team members. When a team member accepts an invitation, a card appears on the Team page of ProSoft Connect.

1. Click on the **Edit Access** option.

2. This opens the access dialog for the new team member. Initially, access defaults to "Connect only" which means that that user is allowed to create a tunnel, but is not allowed to configure a gateway.

3. Change this user's access rights by clicking on any of the first 3 access selections and then click the **Save Access** button.
5.5 Changing Firmware

You can schedule a firmware change for multiple gateways or a single gateway through ProSoft Connect. There are two ways to start the firmware change process:

i. Click the firmware CHANGE hyperlink in the Device Details block.

![Image showing the firmware CHANGE hyperlink in the Device Details block.]

ii. Select CHANGE FIRMWARE from the setup icon in the top-right corner of every configuration page.

![Image showing the CHANGE FIRMWARE option in the setup menu.]

1 Click on the **CHANGE FIRMWARE** option to open the *Firmware Upgrade* dialog.

![Firmware Upgrade Dialog]

This dialog lists the most recent firmware versions and details about this version.

2 Select the version that you want to install by clicking the correct version's radio button.

![Select Version]

At this point, you have two options:

i. **Change Now** - Allows you to select additional gateways for upgrade and then immediately performs the upgrade.

ii. **Schedule for Later** - Allows you to select additional gateways for upgrade and then allows you to schedule a date and time for the upgrade to occur.
**Change Now**

1. With the correct firmware version selected, click the **CHANGE NOW** button. You are prompted as to whether or not you want to upgrade other gateways.

   ![Firmware Upgrade](image)

   **Upgrade other gateways?**

<table>
<thead>
<tr>
<th>Name</th>
<th>Serial Number</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLX35-NB2-TEST1</td>
<td>00:0D:80:A2:BE:28</td>
<td>1.4.50-r0</td>
</tr>
<tr>
<td>PLX35-NB2-TEST2</td>
<td>00:0D:80:A3:08:B4</td>
<td>1.4.50-r0</td>
</tr>
</tbody>
</table>

   - [Cancel](#)  
   - [This Gateway and Selected](#)  
   - [Only This Gateway](#)

2. Choose any available gateways that you want to upgrade, if applicable.

3. Click the **APPLY ONLY TO THIS GATEWAY** button if you have do not need to upgrade additional gateways or click the **APPLY TO THIS GATEWAY AND SELECTED** button to upgrade firmware on the current gateway and any selected gateways.

4. The firmware upgrade starts immediately.

**Schedule for Later**

1. With the correct firmware version selected, click the **SCHEDULE FOR LATER** button. You are prompted as to whether or not you want to schedule upgrades for other gateways.

   ![Firmware Upgrade](image)

   **Schedule upgrade for other gateways?**

<table>
<thead>
<tr>
<th>Name</th>
<th>Serial Number</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLX35-NB2-TEST1</td>
<td>00:0D:80:A2:83:28</td>
<td>1.4.50-r0</td>
</tr>
<tr>
<td>PLX35-NB2-TEST2</td>
<td>00:0D:80:A3:08:B4</td>
<td>1.4.50-r0</td>
</tr>
</tbody>
</table>

   - [Cancel](#)  
   - [This Gateway and Selected](#)  
   - [Only This Gateway](#)
2  If you don't want to schedule upgrades for other gateways, click the **APPLY ONLY TO THIS GATEWAY** button to schedule the upgrade.

3  Schedule the date and time for the firmware change to occur.

4  Click the **SCHEDULE** button.

5  If you want to schedule changes for other gateways, use the **APPLY TO THIS GATEWAY AND SELECTED** button and follow the same procedure.
6 Ethernet Cable Specifications

ProSoft recommends using a category 5 (or better) Ethernet cable with the PLX35-NB2. A category 5 cable has four twisted pairs of wire that are color-coded and cannot be swapped. The gateway only uses two of the four pairs when running at 10 MBit or 100 MBit speeds.

The Ethernet port on the gateway automatically detects the network speed and cable type and uses the appropriate pins to send and receive Ethernet signals. Use either a standard Ethernet straight-through cable or a crossover cable when connecting the gateway to an Ethernet hub, a 10/100/1000 Base-T Ethernet switch, or directly to a PC.

6.1 Ethernet Cable Configuration

Note: The standard connector view shown is color-coded for a straight-through cable.

<table>
<thead>
<tr>
<th>Crossover cable</th>
<th>Straight-through cable</th>
</tr>
</thead>
<tbody>
<tr>
<td>RJ-45 PIN</td>
<td>RJ-45 PIN</td>
</tr>
<tr>
<td>1 Rx+</td>
<td>3 Tx+</td>
</tr>
<tr>
<td>2 Rx-</td>
<td>6 Tx-</td>
</tr>
<tr>
<td>3 Tx+</td>
<td>1 Rx+</td>
</tr>
<tr>
<td>6 Tx-</td>
<td>2 Rx-</td>
</tr>
</tbody>
</table>

Pin #1

Crossover cable

1 Rx+ 2 Rx- 3 Tx+ 6 Tx-

Straight-through cable

1 Rx+ 1 Tx+ 2 Tx- 3 Tx+ 6 Tx- 6 Rx-
7 Support, Service & Warranty

7.1 Contacting Technical Support

With ProSoft Connect, you may click on the Support link at any time to initiate a chat with Support about issues in ProSoft Connect, or gateways managed by ProSoft Connect.

ProSoft Technology, Inc. is committed to providing the most efficient and effective support possible. Before calling, please gather the following information to assist in expediting this process:

1. Product Version Number
2. System architecture
3. Network details

If the issue is hardware related, we will also need information regarding:

1. Module configuration and associated ladder files, if any
2. Module operation and any unusual behavior
3. Configuration/Debug status information
4. LED patterns
5. Details about the interfaced serial, Ethernet or Fieldbus devices

**Note:** For technical support calls within the United States, ProSoft’s 24/7 after-hours phone support is available for urgent plant-down issues.
7.2 Warranty Information

For complete details regarding ProSoft Technology’s TERMS & CONDITIONS OF SALE, WARRANTY, SUPPORT, SERVICE AND RETURN MATERIAL AUTHORIZATION INSTRUCTIONS, please see the documents at: www.prosoft-technology.com/legal

For additional ProSoft Technology contacts in your area, please visit: https://www.prosoft-technology.com/About-Us/Contact-Us.
Index

A
About the PLX35-NB2 Network Bridge • 6
Adding Team Members • 61
Agency Approvals and Certifications • 3

C
Cloud-based Management using ProSoft Connect • 50
Connecting to the PLX35-NB2 Web Page • 14, 50
Contacting Technical Support • 8, 69
Content Disclaimer • 2
Create a new VPN Client • 54

E
Editing Team Member Access • 63
Ethernet Cable Configuration • 68
Ethernet Cable Specifications • 68
Exporting a Configuring File • 45

H
How to Contact Us • 2

I
Important Installation Instructions • 3
Installing the PLX35-NB2 • 11

J
Jumper Information • 8

L
LED Indicators • 12
Local Configuration using the Gateway's Configuration Webpage • 14, 60
Login and Activate ProSoft Connect • 50

P
PLX35-NB2 Package Contents • 8

R
Rebooting the Gateway • 47

S
Setting Gateway Configuration Parameters • 16
Specifications • 7
Start Here • 6
Support, Service & Warranty • 69

U
Updating Firmware • 64
Updating the Gateway's Firmware (NB2) • 46
Using ProSoft Connect to Configure the PLX35-NB2 • 60

V
Verifying the VPN Connection • 58
Viewing Gateway Logfile Activity (NB2) • 43
Viewing the Overview Page • 15

W
Warranty Information • 70

Y
Your Feedback Please • 2